IN THE CLAIMS:

Please amend the claims as set forth below:

1. (Currently Amended) A method ~~of~~ for verifying the validity of ~~generating~~ an encrypted code generated in base L, comprising the steps ~~of~~:

obtaining an encrypted code fashioned as a base L string derived from ~~providing~~ an n-bit raw number by ~~;~~

~~producing a first string through application of~~ ~~applying~~ a one-way hash function ~~on~~ to the n-bit raw number with a first secret key, ~~to generate a first strung;~~

~~designating~~ an m-bit portion of the first string as an m-bit validation number, ~~; and~~

~~producing a second string through combination of~~ ~~combining~~ the m-bit validation number and the n-bit raw number ~~to generate a second string,~~ producing a third string through application of an encryption algorithm to the second string with a second secret key, and converting the third string to the base L string;

converting the base L string to a base 2 string;

decrypting the base 2 string; and

verifying the validity of the encrypted code by processing the decrypted base 2 string.

2. (Currently Amended) The method of claim 1, ~~further comprising~~ ~~the steps~~ wherein the encryption algorithm is ~~of:~~

~~applying~~ a DES3 encryption algorithm ~~to the second string with a second secret key to generate a third string; and~~

~~converting the third string to base L to generate the encrypted code.~~

3. (Original) The method of claim 1, wherein n=32, m=16, and L=29.

4. (Original) The method of claim 1, wherein the one-way hash function is MD5.

5. (Currently Amended) The method of claim 1, wherein the combination step ~~of combining~~ includes concatenating the m-bit validation number and the n-bit raw number.

6. (Original) The method of claim 1, wherein the m-bit validation number is the m most significant bit (MSB) portion of the second string.

1   7.   (Currently Amended) The method of claim 1, wherein the m-bit validation number is the m most

2 significant bit (MSB) portion of the first string.

1   8.   (Currently Amended) A method of verifying the ~~valifdity~~ validity of a code obtained by a user

2 from an object, comprising the steps of:

3   ——————generating a code with encrypted information;

4   ——————fixing the code on an object to be distributed to a user;

5   ——————obtaining the code from the object, by the user;

6   receiving the code ~~on-line~~on-line from the user, the code is generated with encrypted information

7 as a base L string and obtained by the user off-line from the object;

8   converting the base L string to a base 2 string;

9   decrypting the base 2 string; and

10   verifying the validity of the code by processing the ~~encrypted information~~decrypted base 2 string.

1   9.   (Currently Amended) The method of claim 8, wherein the code is generated by~~step of generating~~

2 ~~includes the steps of~~:

3   providing an n-bit raw number;

4   generating a first string through application of ~~applying~~a one-way hash function ~~on~~to

5 the n-bit raw number with a first secret key~~to generate a first string~~;

6   designating a m-bit portion of the first string as an m-bit validation number;

7   generating a second string by combining the m-bit validation number and the n-bit raw

8 number~~to generate a second string~~;

9   generating a third string through application of~~applying~~ a DES3 encryption algorithm to

10 the second string with a second ~~secet~~secret key~~to generate a third string~~; and

11   producing the code with the encrypted information by converting the third string to a base L

12 string~~to generate the code with the encrypted information~~.

1   10.   (Currently Amended) The method of claim ~~9~~1, wherein the decryption of the base 2 string is

2 performed through application of a reverse DES3 encryption algorithm with the second secret key which

3 produces a second test code, and wherein the step of verifying further includes ~~the steps of~~:

4   ——————converting the code in base L to generate a first test code in base 2;

5 ───────decrypting the first test code with the second secret key using a reverse DES3 encryption

6 algorithm to generate a second test code;

7 ───────generating a third test code through application of~~applying~~ the one-way hash algorithm to the

8 second test code ~~to generate a third test code~~; and

9 ───────comparing a designated m-bit portion of the second test code to a designated m-bit portion of

10 the third test code~~,~~ and declaring the code valid if the comparison is positive~~, declaring the code to be valid~~.

1 11. (Original) The method of claim 10, wherein the m-bit validation number is the m-most

2 significant bit (MSB) of the first string in the generating step and the designated m-bit portion is the most

3 significant bit portion of the second test code in the comparing step.

1 12. (Currently Amended) A method for awarding incentive points to a user, comprising the steps of:

2 ~~generating a code with encrypted information;~~

3 ───~~providing the code to an entity for printing on an object;~~

4 receiving on-line~~the code~~ from a user ~~on-line, the~~ a code ~~having been~~ generated with encrypted

5 information and obtained by the user off~~-ret鋀ived from the object by the user~~;

6 verifying the validity of the code by processing the encrypted information; and

7 awarding incentive points to the user if the code is valid.

1 13. (Currently Amended) The method of claim 12, wherein the code is generated by~~step of~~

2 ~~generating includes the steps of~~:

3 providing an n-bit raw number;

4 generating a first string through application of~~applying~~ a one-way hash function on~~-to~~ the

5 ~~en-bit~~n-bit raw number with a first secret key ~~to generate a first string~~;

6 designating an m-bit portion of the first string as an m-bit validation number;

7 generating a second string through combination of~~combining~~ the m-bit validation number

8 and the n-bit raw number ~~to generate a scond string~~;

9 generating a third string through application of~~applying~~ a DES3 encryption algorithm to

10 the second string with a second secret key ~~to generate a third string~~; and

11 producing the code with the encrypted information through conversion of~~converting~~ the

12 third string to a base L string~~to generate atch code with the encrypted information~~.

1 14. (Currently Amended) The method of claim ~~13~~12, wherein the step of verifying includes:

2   generating a first test code by converting the ~~code in~~ base L string of the code to a base 2

3   string~~generate a first test code in base 2~~;

4   generating a second test code by decrypting the first test code with the second secret key using a

5   reverse DES3 encryption algorithm ~~to generate a second test code~~;

6   generating a thirst test code by applying the one-way hash algorithm to the second test code ~~to~~

7   ~~generate a third test code~~; and

8   determining the validity of the code by comparing a designated m-bit portion of the second test

9   code to a designated m-bit portion of the third test code~~, and if the comparison is positive, declaring the~~

10   ~~code to be valid~~.

1   15.   Canceled

1   16.   (Currently Amended) The method of claim ~~15~~14, wherein the m-bit validation number is the m most

2   significant bit (MSB) of the first string in the generating step and the designated m-bit portion is the most

3   significant bit portion of the second test code and third test code in the comparing step.

1   17.   (Currently Amended) An offline-online points system, comprising:

2   a main server configured ~~for providing a user~~ with an interface ~~to~~ for ~~submit~~receiving a code from a

3   user, wherein the code is obtainable by the user ~~offline~~off-line and is associated with N points, wherein each

4   point, characterized as a purchase or attention incentive point, is redeemable and maintainable in an account

5   for the user; and

6   a code server configured for maintaining valid codes and verifying, against the valid codes, the

7   validity of ~~that~~ the code ~~submitted by~~received from the user, wherein the account has a balance of points

8   capable of growing ~~is valid such that a balance in the account for the user is increased~~ by a predetermined

9   number of points if the code is valid.~~;~~

10   —————— ~~means for generating the code; and~~

11   —————— ~~means for fixing the code onto a medium such that the code is obtainable from the medium offline.~~

1   18.   (Currently Amended) The ~~offline-online points system~~method of claim ~~17~~12, wherein the code is

2   generated by:~~wherein the means for generating the code includes~~

3   ~~means for~~providing a number portion,

4   ~~means for~~deriving a validation portion from the number portion,

5   ~~means for~~appending the validation portion to the number portion to form a string,

6   ~~means for~~ encrypting the string, and

7   ~~means for~~ deriving the code from the encrypted string by converting the encrypted string to

8 base L string.

1   19.   (Currently Amended) The ~~offline online points system~~ method of claim 18, wherein the code is a

2 fixed-length string with C characters, and wherein the ~~means for~~ step of deriving the code further includes

3 ~~means for~~ prepending a character to the base L string any number of times that is needed to achieve the

4 fixed-length of C characters.

1   20.   (Currently Amended) The ~~offline online points system~~ method of claim 18, wherein L is the

2 number of characters in the alphabet.

1   21.   (Currently Amended) The ~~offline online points system~~ method of claim 18, wherein the string is

2 48-bits long and the number portion is 32-bits long.

1   22.   (Currently Amended) The ~~offline online points system~~ method of claim ~~17~~ 12, wherein the code is

2 generated by: ~~wherein the means for generating the code includes~~

3   ~~means for~~ providing a number portion, $S1_{INT}$, from a first string, S1

4   ~~means for~~ arranging a first secret key, K1, next to the number portion, $S1_{INT}$, from S1, to

5 form a second string, S2,

6   ~~means for~~ applying a hash function to S2 to produce a third string, S3,

7   ~~means for~~ extracting a validation portion, $S1_{VAL}$, from S3 and arranging $S1_{VAL}$, next to

8 $S1_{INT}$ in S1 ($S1 = S1_{VAL} + S1_{INT}$),

9   ~~means for~~ encrypting S1 using a second secret key, K2, to form a fourth string, S4, and

10   ~~means for~~ deriving the code by converting S4 to a base L fixed-length code string.

1   23.   (Currently Amended) The ~~offline online points system~~ method of claim 22, wherein the first and

2 second secret keys, K1 and K2, are 128-bits long and the encryption ~~means~~ includes DES3 encryption

3 algorithm.

1   24.   (Currently Amended) The ~~offline online points system~~ method of claim 22, wherein the hash

2 function ~~application means has~~ includes MD5, a one-way hash algorithm.

1 25. (Currently Amended) The ~~offline-online points system~~method of claim 22, wherein S1 is 48-bits

2 long and the number portion, $S1_{INT}$, is 32-bits long.

1 26. (Currently Amended) The offline-online points system of claim 17, wherein for verifying the

2 ~~submitted~~ code received from the user the code server includes~~:~~:

3   means for converting the ~~submitted~~ code from a base L string into a base 2 string, $S4_{BASE2}$~~:~~;

4   means for decrypting $S4_{BASE2}$ using a second secret key, K2, to form a decrypted first string,

5            $S1'$~~:~~;

6   means for providing a number portion, $S1'_{INT}$, from $S1'$;

7   means for arranging a first secret key, K1, next to the number portion, $S1'_{INT}$, from S1, to

8   form a second string, $S2'$~~:~~;

9   means for applying a hash function to S2' to form a third string $S3'$~~:~~;

10   means for extracting a validation portion from S3' and a validation portion from $S1'$~~,~~; and

11   means for determining if the code is valid by comparing the validation portion from S3' with

12   the validation portion from S1'.

1 27. (Original) The offline-online points system of claim 26, wherein S3' and S1 are each 48-bits long

2 and the secret keys, K1 and K2 are 128-bits long.

1 28. (Currently Amended) The offline-online points system of claim 26, wherein the decryption means

2 includes $DES3^{-1}$ decryption algorithm means and the hash function application means includes MD5 hash

3 algorithm means.

1 29. (Currently Amended) A method for offline-online ~~handling~~ management of incentive points,

2 comprising:

3   receiving ~~generating~~ a code~~, wherein~~ wherein the code is generated by providing a number portion,

4 deriving a validation portion from the number portion, appending the validation portion to the number

5 portion to form a string, encrypting the string, and deriving the code from the encrypted string by converting

6 the encrypted string to base L string, the code obtained off-line and received on-line; and

7   processing the code.

8 ~~fixing the code onto a medium such that the code is obtainable from the medium offline.~~

1   30.   (Currently Amended) The method of claim 29, ~~further comprising~~wherein processing the code

2   includes:

3   ~~obtaining the code offline;~~

4   submitting the code ~~online~~ to a server that has valid codes, wherein the code is associated with N

5   points maintained by the server in a user account, wherein each point, characterized as a purchase or

6   attention incentive point, is redeemable; and

7   verifying the ~~submitted~~ code against the valid codes to determine if it is valid, wherein if the

8   ~~submitted~~ code is valid, a predetermined number of points are added to the user account.

1   31.   (Original) A method as in claim 29, wherein the code is a fixed-length string with C characters,

2   and wherein a character is prepended to the base L string any number of times that is needed to achieve

3   the fixed-length of C characters.

1   32.   (Original) A method as in claim 29, wherein L is the number of characters in the alphabet.

1   33.   (Original) A method as in claim 29, wherein the string is 48-bits long and the number portion is

2   32-bits long.

1   34.   (Currently Amended) A method for offline-online ~~handling~~ management of incentive points,

2   comprising:

3   generating a code by:

4   providing a number portion, $S1_{INT}$, from a first string, $S1$,

5   arranging a first secret key, K1, next to the number portion, $S1_{INT}$, from S1, to form a

6   second string, S2,

7   applying a hash function to S2 to produce a third string, S3,

8   extracting a validation portion, $S1_{VAL}$, from S3 and arranging $S1_{VAL}$, next to $S1_{INT}$ in S1

9    $(S1=S1_{VAL}+ S1_{INT})$,

10   encrypting S1 using a second secret key, K2, to form a fourth string, S4, and

11   deriving the code by converting S4 to a base L fixed-length code string; and

12   fixing the code onto a medium such that the code is obtainable from the medium ~~offline~~off-line.

1   35.   (Currently Amended) A method as in claim 34, wherein the first and second secret keys, K1 and

2   K2, are 128-bits long and the encryption involves a_DES3 encryption algorithm.

1　36.　(Original) A method as in claim 34, wherein the hash function is MD5, a one-way hash algorithm.

1　37.　(Original) A method as in claim 34, wherein S1 is 48-bits long and the number portion, $S1_{INT}$, is 32-
2　bits long.

1　38.　(Original) A method as in claim 30 wherein the step of verifying the submitted code includes,
2　　　　　converting the submitted code from a base L string into a base 2 string, $S4_{BASE2}$,
3　　　　　decrypting $S4_{BASE2}$ using a second secret key, K2, to form a decrypted first string, S1',
4　　　　　providing a number portion from S1'
5　　　　　arranging a first secret key, K1, next to the number portion from S1' to form a second string,
6　　　S2',
7　　　　　applying a hash function to S2' to form a third string S3',
8　　　　　extracting a validation portion from S3' and a validation portion from S1', and
9　　　　　determining if the code is valid by comparing the validation portion from S3' with the
10　　　　　validation portion from S1'.

1　39.　(Original) A method as in claim 38, wherein S3' and S1 are each 48-bits long and the secret keys, K1
2　and K2 are 128-bits long.

1　40.　(Currently Amended) A method as in claim 38, wherein the decryption involves the DES3^{-1}
2　decryption algorithm and the ~~has~~ hash function involves the MD5 hash algorithm.